

## **[Portal Fidelización] Guía de despliegue Zero**

**PREPARADO POR:**

**PRAGMA S. A.**

**PARA:**

**ATH**

## Lista de cambios

Fecha	Versión	Descripción	Autores
08-03-2018	1.0	Manual de paso entre ambientes y configuraciones iniciales del proyecto.	Augusto Cardona Giraldo Carlos Andres Cardona
02-04-2018	1.1	Configuraciones adicionales para lectura de atributos desde puma.	Carlos Cardona
13-04-2018	1.2	Outbound connections (Ajax Proxy) y preferencias de portlets.	Carlos Cardona

## [Introducción](#)

### [0. Scripts iniciales base de datos](#)

#### [1. Configurar Custom User Repository \(CUR\)](#)

[1.1. Permitir operaciones si algunos de los repositorios están caídos](#)

[1.2. Copiar las clases que implementan el CUR](#)

[1.3. Reiniciar el servidor](#)

[1.4. Configuraciones globales de seguridad del WAS](#)

[1.5. Añadir un CUR como parte de un conjunto de repositorios federados](#)

[1.6. Probar la configuración](#)

#### [2. Portal Virtual](#)

#### [3. Temas y skins](#)

[3.1. Importar Temas y Skins](#)

[3.2. Desplegar temas en WebDAV](#)

#### [4. Sindicación](#)

[4.1. Preparación para la sindicación hacia un cluster](#)

[4.2. Procedimiento de establecimiento de la sindicación](#)

[4.3. Permisos en las bibliotecas de contenido](#)

[4.4. Errores comunes de la sindicación](#)

[4.4.1. Elementos fallidos](#)

[4.4.2. Sindicador bloqueado](#)

[4.4.3. Error de conexión entre el sindicador y el suscriptor](#)

#### [5. Portlets](#)

[5.1. Importar portlets desde el servidor \(WebMod\)](#)

[5.2. Importar portlets desde el servidor <ServidorDestino> XML](#)

#### [6. Procedimientos adicionales](#)

[6.1. Configuración Portlets Scripts \(Angular\)](#)

[6.2 outbound connections \(Ajax Proxy\)](#)

[6.2.1. Correlación de servlet](#)

[6.2.2. Configurar el proxy](#)

[6.2.3. Actualizar la configuración del proxy](#)

[6.2.4. Otros comandos utilitarios son](#)

[6.3. Editar preferencias de Portlets](#)

[6.3.1 Preferencia url Aviatour](#)

[6.4. Configurar preferencias en el servidor de aplicaciones](#)

## [7. Anexos](#)

[7.1. Configuración del idioma](#)

[7.2. Limpieza de caché tema:](#)

[7.3. Permisos miga de pan](#)

## [8. Configuración Kubernetes](#)

[8.1. Borrar los deployment y services ya creados](#)

[8.1.1 config-api](#)

[8.1.2 api-gateway](#)

[8.1.3 authentication-api](#)

[8.1.4 notificaciones-api](#)

[8.1.5 cuenta-api](#)

[8.1.6 extracto-api](#)

[8.1.7 otp-api](#)

[8.1.8 redenciones-api](#)

[8.2. Copiar los .zip en el servidor de docker](#)

[8.3. Compilar las imágenes de docker](#)

[8.3.1 config-api:v](#)

[8.3.3 authentication-api:v](#)

[8.3.4 notificaciones-api:v](#)

[8.3.5 cuenta-api:v](#)

[8.3.6 api-gateway:v](#)

[8.3.7 extracto-api:v](#)

[8.3.8 otp-api:v](#)

[8.3.9 redenciones-api:v](#)

[8.4. Secrets](#)

[8.5. Validar que el despliegue fue correcto](#)

## Introducción

El presente documento describe el procedimiento de despliegue de un portal en IBM WebSphere Portal. Moviendo los contenidos de un servidor de origen a un servidor de destino.

IBM WebSphere Portal y Web Content Manager consiste en muchos elementos y componentes. Estos incluyen portlets, themes y skins, páginas, eventos, configuraciones de portlet, contenido web y reglas de personalización. Este manual contiene los pasos para mover estos elementos de un ambiente a otro de forma controlada.

## 0. Scripts iniciales base de datos

Descomprimir el .zip y ejecutar los siguientes scripts en los esquemas de Fidelización en la base de datos de qa

- TAPLICACIONES.zip
- TAUDITORIA.zip
- TAUDITORIA.zip
- TPROPIEDADES.zip
- TSAPI\_RECURSOS.zip
- TSAPI\_RESTRICCIONES.zip
- TSAPI\_SESIONES.zip
- TSESION.zip
- TUSUARIOS.zip

## 1. Configurar Custom User Repository (CUR)

Componente de software que implementa las operaciones básicas de un repositorio estándar de usuarios, como lo son la consulta de usuarios, la verificación de contraseñas y la consulta de grupos, sobre un repositorio no estándar, aclarando que para el WAS, un repositorio no estándar es cualquier cosa que no sea un LDAP o una BD que no se adecúe a unos lineamientos de estructura.

### ***1.1. Permitir operaciones si algunos de los repositorios están caídos***

Ingresar a la consola administrativa de WAS, e ir a Security / Global security / Configurar

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Jobs
- Services
- Resources
- Runtime Operations
- Security**
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
  - JAX-WS and JAX-RPC security runtime
- Operational policies
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard    Security Configuration Report

**Administrative security**

☒ Enable administrative security

- [Administrative user roles](#)
- [Administrative group roles](#)
- [Administrative authentication](#)

**Application security**

☒ Enable application security

**Java 2 security**

☐ Use Java 2 security to restrict application access to local resources

- ☒ Warn if applications are granted custom permissions
- ☐ Restrict access to resource authentication data

**User account repository**

Realm name: defaultWIMFileBasedRealm

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

[Configure...](#) [Set as current](#)

**Authentication**

Authentication mechanisms and expiration

☒ LTPA

- ☐ Kerberos and LTPA
- [Kerberos configuration](#)
- [Authentication cache settings](#)
- ☐ Web and SIP security
- ☐ RMI/IIOP security
- ☐ Java Authentication and Authorization Service
- ☐ Enable Java Authentication SPI (JASPI)
  - [Providers](#)
- ☐ Use realm-qualified user names
  - [Security domains](#)
  - [External authorization providers](#)
  - [Programmatic session cookie configuration](#)
  - [Custom properties](#)

Chulear la casilla con el nombre: **Allow operations if some of the repositories are down**

☒ Ignore case for authorization

☒ **Allow operations if some of the repositories are down**

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
<input type="checkbox"/>	<a href="#">dc=pragma,dc=com,dc=co</a>	<a href="#">pragma_AD</a>	LDAP:AD
<input type="checkbox"/>	<a href="#">o=afiliados</a>	<a href="#">RepositorioAfiliados</a>	Custom
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 3			

## 1.2. Copiar las clases que implementan el CUR

Al classpath bootstrap del WAS. Para hacerlo, basta con copiar dichas clases (normalmente empaquetadas en uno o más archivos .jar) y todas sus dependencias al directorio <WAS\_HOME>/lib/ext. Por ejemplo,



/app/wpadmin1/IBM/WebSphere/AppServer/lib/ext/			
Name	Size (KB)	Last modified	Owner
..			
custom-repositorio.jar	57	2018-03-15 ...	wpadr
ojdbc6.jar	2 675	2018-03-15 ...	wpadr
wp.auth.base.sua_loginmodul...	6	2016-12-08 ...	wpadr
wp.auth.base.sua_RedirectS...	5	2016-12-08 ...	wpadr
wp.auth.tai.jar	116	2016-12-08 ...	wpadr
wps.properties	1	2016-12-08 ...	wpadr

Las dependencias están adjuntas en esta guía, son:

- custom-repositorio.jar
- ojdbc8.jar

NOTA: Para ambientes en clúster se copian en cada nodo.

### 1.3. Reiniciar el servidor

En este punto, reiniciar el servidor para que este cargue las clases y poder realizar las configuraciones que vienen a continuación, pues algunas de estas ya van a necesitar de las clases.

### 1.4. Configuraciones globales de seguridad del WAS

Ingresar a la consola administrativa de WAS, e ir a Security / Global security / Configure

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Jobs
- Services
- Resources
- Runtime Operations
- Security**
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
  - JAX-WS and JAX-RPC security runtime
- Operational policies
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard    Security Configuration Report

**Administrative security**

☒ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

**Application security**

☒ Enable application security

**Java 2 security**

☐ Use Java 2 security to restrict application access to local resources

- Warn if applications are granted custom permissions
- Restrict access to resource authentication data

**User account repository**

Realm name: defaultWIMFileBasedRealm

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

**Authentication**

Authentication mechanisms and expiration

☒ LTPA

☐ Kerberos and LTPA

- Kerberos configuration
- Authentication cache settings
- Web and SIP security
- RMI/IIOP security
- Java Authentication and Authorization Service

☐ Enable Java Authentication SPI (JASPI)

- Providers

☐ Use realm-qualified user names

- Security domains
- External authorization providers
- Programmatic session cookie configuration
- Custom properties

Ir a la opción “Manage repositories” que aparece en el grupo de configuraciones etiquetado como “Related items”.

- ☒ Ignore case for authorization
- ☐ Allow operations if some of the repositories are down

Repositories in the realm:

Add repositories (LDAP, custom, etc)... Use built-in repository Remove			
Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
<input type="checkbox"/>	<a href="#">dc=pragma,dc=com,dc=co</a>	<a href="#">pragma_AD</a>	LDAP:AD
<input type="checkbox"/>	<a href="#">o=defaultWIMFileBasedRealm</a>	InternalFileRepository	File
Total 2			

Related Items

Additional Properties

- [Property extension repository](#)
- [Entry mapping repository](#)
- [Supported entity types](#)
- [User repository attribute mapping](#)
- [Custom properties](#)

▪ [Manage repositories](#)

- [Trusted authentication realms - inbound](#)

En el botón desplegable “Add”, seleccionar “Custom repository”.

[Global security](#) > [Federated repositories](#) > [Manage repositories](#)

Repositories that are configured in the system are listed in the following table. You can add or delete external repositories.

⊕ Preferences

Add ▾ Delete		
LDAP repository		
Custom repository		
File repository		
Select	Repository Identifier ▾	Repository Type ▾
You can administer the following resources:		
	<a href="#">InternalFileRepository</a>	File
<input type="checkbox"/>	<a href="#">pragma_AD</a>	LDAP:AD
Total 2		

Diligenciar y/o editar el formulario de la siguiente manera:

- Repository identifier: RepositorioAfiliados
- Repository adapter class name:  
[co.com.ath.fidelizacion.portal.custom.vmm.AdaptadorRepositorioAfiliados](#)

## Custom properties según el ambiente

Ambiente	Pruebas Técnicas	QA	Producción
<b>username</b>	<i>FIDELIZACION</i>	<i>FIDELIZACION</i>	<i>FIDELIZACION</i>
<b>password</b>	<i>Fidelizacion_20_xx</i>	<i>Fidelizacion_20_xx</i>	<i>&lt;passwordProd&gt;</i>
<b>url</b>	<i>jdbc:oracle:thin:@//10.130.3.229:1528/FIDAVAl</i>	<i>jdbc:oracle:thin:@//scanfdlbdcorqa:1528/FIDAVAl</i>	<i>jdbc:oracle:thin:@//scanfdlbdcorpr:1528/FIDAVAl</i>

### Custom properties:

- **username:** Usuario de la base de datos según el ambiente (Ver tabla anterior).
- **password:** Clave de la base de datos según el ambiente (Ver tabla anterior).
- **url:** jdbc de la base de datos según el ambiente (Ver tabla anterior).
- **registryImplClass:** co.com.ath.fidelizacion.portal.custom.RepositorioUsuarios. clase que proporciona los métodos del repositorio
- **atributo.cn:** nombres
- **atributo.sn:** apellidos
- **atributo.displayName:** displayName
- **atributo.numeroDocumento:** numeroDocumento
- **atributo.tipoDocumento:** tipoDocumento
- **atributo.uid:** idUsuario

### General Properties

\* Repository identifier

RepositorioAfiliados

\* Repository adapter class name

co.com.ath.fidelizacion.portal.custom.vmm.AdaptadorRepositorioAfiliados

Federated repository properties for login

Custom properties

New

Edit

Delete

Select	Name	Value
<input type="checkbox"/>	password	*****
<input type="checkbox"/>	atributo.cn	nombres
<input type="checkbox"/>	atributo.sn	apellidos
<input type="checkbox"/>	atributo.displayName	displayName
<input type="checkbox"/>	atributo.numeroDocumento	numeroDocumento
<input type="checkbox"/>	atributo.tipoDocumento	tipoDocumento
<input type="checkbox"/>	atributo.uid	idUsuario
<input type="checkbox"/>	url	jdbc:oracle:thin:@dbmed14.pragma.com.co:1521:orcutf8
<input type="checkbox"/>	registryImplClass	co.com.ath.fidelizacion.portal.custom.RepositorioUsuarios
<input type="checkbox"/>	username	ORAATHFIDELIZACIONQA

Hacer clic en OK y guardar la configuración.

## 1.5. Añadir un CUR como parte de un conjunto de repositorios federados

Agregar este repositorio a una lista de repositorios federados. Para hacerlo, se siguen las siguientes acciones en la misma sección de repositorios federados.

En la lista de repositorios federados, se hace clic en el botón “Add Base entry to Realm...”.

- ☒ Ignore case for authorization
- ☐ Allow operations if some of the repositories are down

Repositories in the realm:

<a href="#">Add repositories (LDAP, custom, etc)...</a> <a href="#">Use built-in repository</a> <a href="#">Remove</a>			
Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
<input type="checkbox"/>	<a href="#">dc=pragma,dc=com,dc=co</a>	<a href="#">pragma_AD</a>	LDAP:AD
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 2			

Se selecciona el repositorio que se desea agregar entre la lista de repositorios previamente creados. Aquí ya debería figurar el repositorio que creamos anteriormente y en el Unique distinguished se ingresa **o=afiliados**.

#### [Global security](#) > [Federated repositories](#) > [Repository reference](#)

Specifies a set of identity entries in a repository that are referenced by a base (or parent) entry into the dir. If multiple repositories or multiple subtrees of the same repository are included in the same realm, it might be additional distinguished names to uniquely identify this set of entries within the realm.

##### General Properties

\* **Repository**

[RepositoryAfiliados](#) [New Repository...](#)

\* **Unique distinguished name of the base (or parent) entry in federated repositories**

[o=afiliados](#)

☐ **Distinguished name in the repository is different**

Distinguished name of a subtree in the main repository

Hacer clic en el botón OK y guardar la configuración, deberá verse así.

Repositories in the realm:

Add repositories (LDAP, custom, etc)... Use built-in repository Remove			
Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
<input type="checkbox"/>	dc=pragma,dc=com,dc=co	pragma_AD	LDAP:AD
<input type="checkbox"/>	o=afiliados	RepositorioAfiliados	Custom
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 3			

## 1.6. Probar la configuración

Verifique inicialmente que el servidor haya iniciado sin errores y que pueda autenticarse a la consola administrativa con el usuario administrativo primario.

Ir a la sección Users and Groups / Manage Groups

Busque alguno de los grupos que sabemos contiene el CUR que creó y verifique que se muestre en el listado. Por ejemplo, en nuestro CUR, sabemos que existe el grupo “AFILIADO\_PUNTOS”.

### Search for Groups

Search by \* Search for \* Maximum results

Group name

1 groups matched the search criteria.

Create... Delete Select Select an action...			
Select	Group name	Description	Unique Name
<input type="checkbox"/>	AFILIADO_PUNTOS		cn=AFILIADO_PUNTOS,o=afiliados
Page 1 of 1 Total: 1			

Ir a la sección Users and Groups / Manage Users

Busque alguno de los usuarios que sabemos que está contenido en el CUR y verifique que se muestra en pantalla. Por ejemplo, en nuestro CUR, sabemos que existe el usuario “AFI\_CC\_1152197588”.

### Search for Users

Search by \* Search for \* Maximum results

User ID

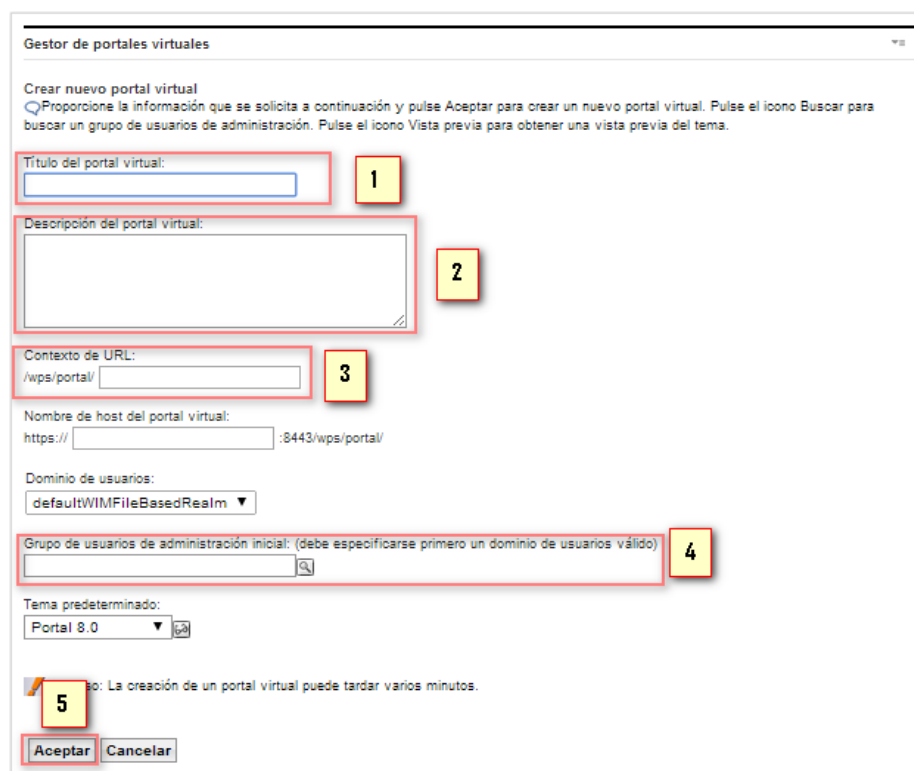
1 users matched the search criteria.

Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	<a href="#">AFI CC 1152197588</a>	Carlos Andrés	Cardona Monsalve	carlos.cardona@pragma.com.co	uid=AFI_CC_1152197588,o=afiliados
Page 1 of 1					Total: 1

## 2. Portal Virtual

A continuación se deben ejecutar los siguientes pasos para la creación del **Portal Lealtad**:

1. En el portal base (<http://<hostname>:<port>/wps/myportal/>) ir a la sección de Administración.
2. Ir a Portales virtuales e ingresar a Gestión de portales virtuales
3. Ir a la opción Nuevo portal virtual y dar clic
4. Diligenciar los campos con los siguientes valores:
  - a. Título del portal virtual: **Portal Lealtad**
  - b. Descripción del portal virtual: **Portal virtual para Portal Lealtad Grupo Aval**
  - c. Contexto de URL: **portal-lealtad**



**Gestor de portales virtuales**

Crear nuevo portal virtual

Proporcione la información que se solicita a continuación y pulse Aceptar para crear un nuevo portal virtual. Pulse el icono Buscar para buscar un grupo de usuarios de administración. Pulse el icono Vista previa para obtener una vista previa del tema.

Título del portal virtual:  **1**

Descripción del portal virtual:  **2**

Contexto de URL: /wps/portal/  **3**

Nombre de host del portal virtual: https://  :8443/wps/portal/

Dominio de usuarios: defaultWIMFileBasedRealm ▼

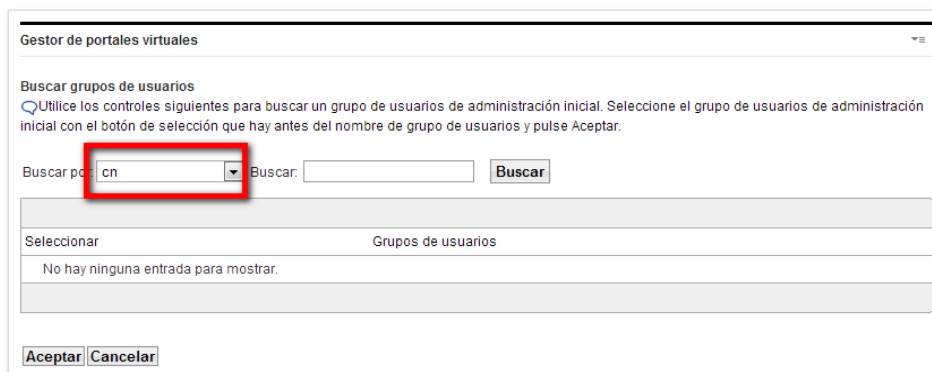
Grupo de usuarios de administración inicial: (debe especificarse primero un dominio de usuarios válido)   **4**

Tema predeterminado: Portal 8.0 ▼

**5** Nota: La creación de un portal virtual puede tardar varios minutos.

**Nota:** En el punto 4 de la imagen, se debe tener claro cuál es el **grupo de administradores** y el respectivo usuario. Con esto claro, se puede seleccionar el Grupo de usuario administradores, así:

1. Dar clic en ícono de la lupa ubicada al lado del campo de texto del punto 4 de la imagen anterior.
2. Seguir las instrucciones dadas en el cuadro de diálogo “Buscar grupos de usuarios” y seleccionar el filtro de búsqueda para definir los usuarios administradores con acceso al portal virtual, regularmente se define **cn**.



**Gestor de portales virtuales**

Buscar grupos de usuarios

Utilice los controles siguientes para buscar un grupo de usuarios de administración inicial. Seleccione el grupo de usuarios de administración inicial con el botón de selección que hay antes del nombre de grupo de usuarios y pulse Aceptar.

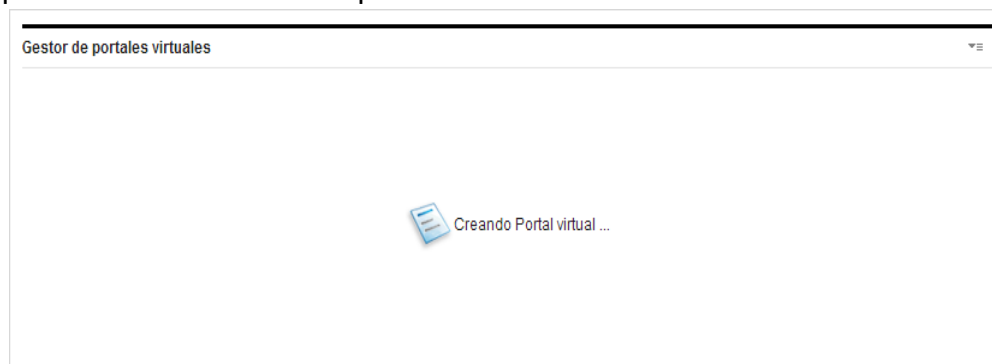
Buscar por:   Buscar:

Seleccionar	Grupos de usuarios
No hay ninguna entrada para mostrar.	

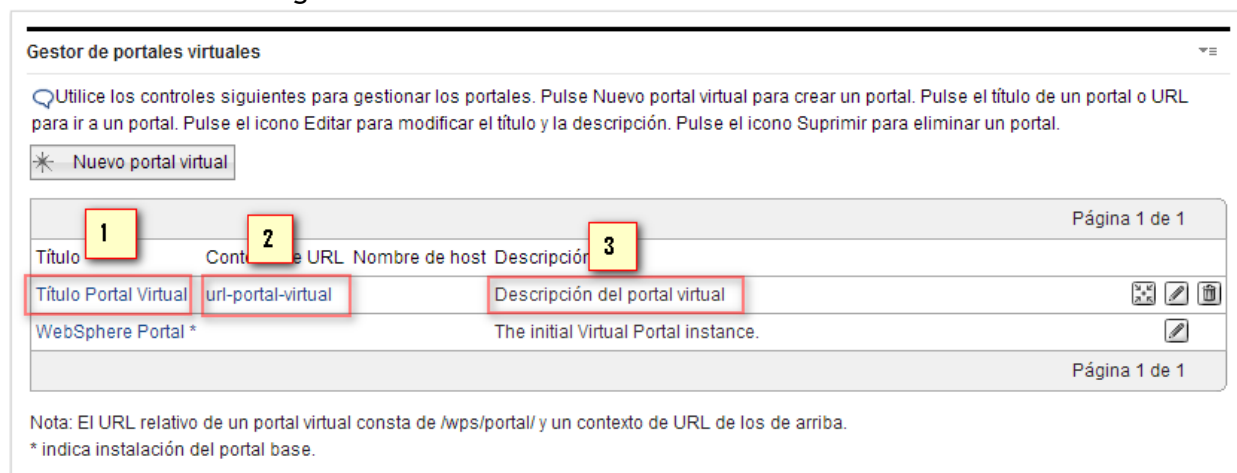
3. Realizar la búsqueda de los usuarios y posteriormente seleccionar el botón de Aceptar



- para que queden definidos como administradores del portal virtual.
4. Clic en aceptar en la ventana “Crear nuevo portal virtual”. Posteriormente el sistema empezará con la creación del portal virtual.



5. Una vez el sistema termina de ejecutar la creación del portal virtual se carga una interfaz similar a la siguiente:



En cuyo caso se debe presentar el título, la URL del portal virtual y la descripción diligenciadas.

## 3. Temas y skins

### 3.1. Importar Temas y Skins

Copiar el xml de los temas desde el servidor *<ServidorOrigen>* al servidor *<ServidorDestino>*:

Inicialmente se debe copiar en un directorio temporal del servidor *<ServidorDestino>* el archivo xml nombrado como *ExportThemesAndSkinsResult.xml* obtenido desde el servidor *<ServidorOrigen>*.

Posteriormente, desde una consola de comandos, ejecutar la siguiente instrucción sobre el servidor *<ServidorDestino>*:

```
/ <RaizInstalaciónPortal>/IBM/wp_profile/PortalServer/bin/xmlaccess.sh           -in  
/ <DirectorioTemporal>/ExportThemesAndSkinsResult.xml                         -out  
/ <DirectorioTemporal>/ResultImport-ExportThemesAndSkinsResult.xml           -url  
http://<hostname>:<port>/wps/config/
```

Del comando anterior se destacan las siguientes variables:

- **<RaizInstalaciónPortal>**: Corresponde con la dirección del servidor donde se encuentra instalado el Portal, regularmente esta dirección electrónica puede estar representada como */appl*, */app* o */usr*.
- **<DirectorioTemporal>**: Corresponde con la dirección del servidor donde se ubica el directorio temporal definido al comenzar la guía de importación de temas y skins.
- **<hostname>**: Dirección del host sobre el que se realizará la importación de los temas y skins, regularmente se proporciona la ip o localhost en caso de estar configurado, si se tiene un nombre de host definido se debe especificar este último.
- **<port>**: Puerto desde el cual responde la aplicación de Portal, regularmente corresponde con 10039, especifique el respectivo.

Si los datos son correctos, el proceso de importación se iniciará y al finalizar, se mostrará el siguiente mensaje informativo, que indica que el procedimiento se ejecutó correctamente:




















EJPXB0020I: The request was processed successfully on the server.

Dicho mensaje estará representado en el archivo xml especificado en el parámetro out del comando.

### 3.2. Desplegar temas en WebDAV

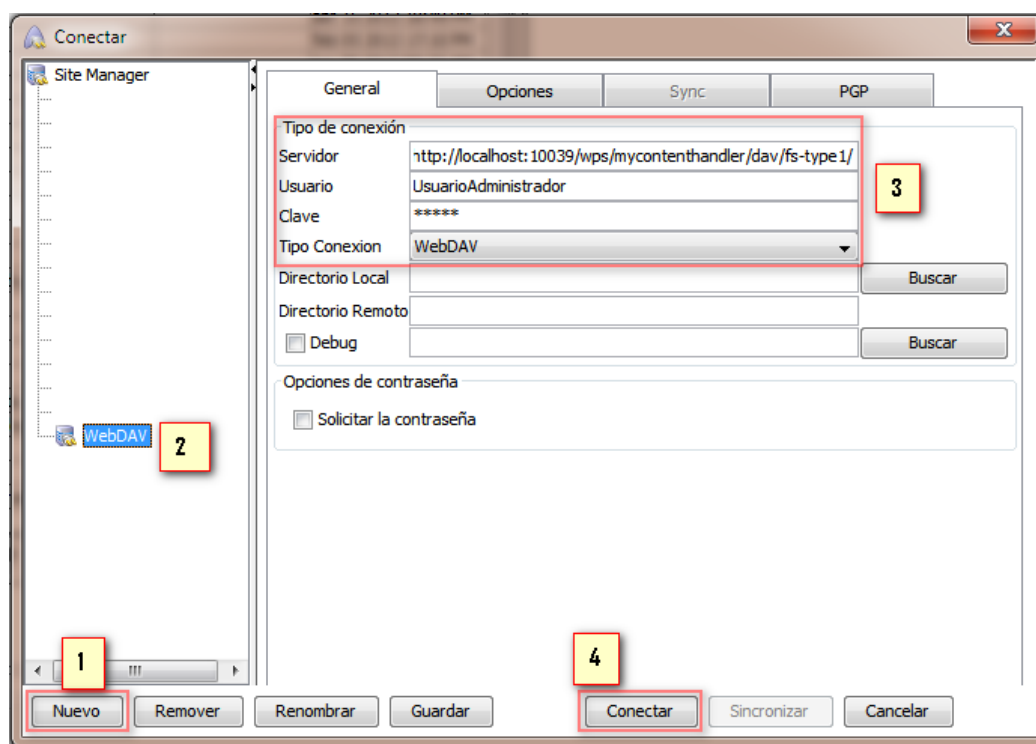
Descomprimir los archivos en formato zip (*TemaFidelizacionAval.zip*) de los temas y skins obtenidos desde el servidor *<ServidorOrigen>*.

Estos recursos de WebDAV deben estar en un directorio de fácil recordación. Los archivos iniciales del tema contemplan la siguiente estructura:

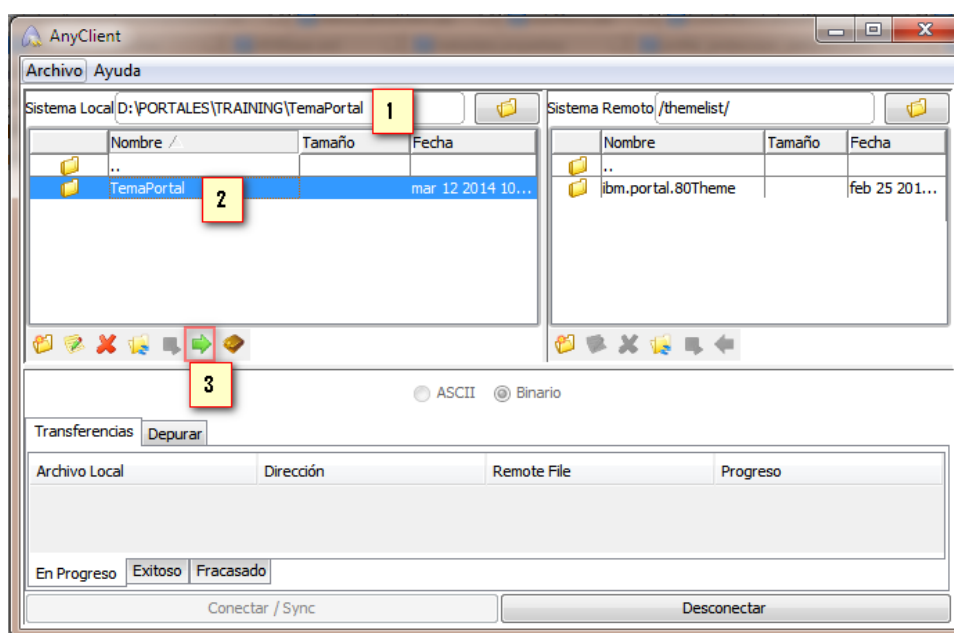
	Nombre	Tamaño	Fecha
	..		
	contributions		mar 11 2014 14:15 PM
	css		mar 11 2014 19:21 PM
	CTC		feb 20 2014 08:52 AM
	images		mar 11 2014 14:37 PM
	js		mar 11 2014 19:20 PM
	layout-templates		feb 20 2014 08:52 AM
	menuDefinitions		feb 20 2014 08:52 AM
	nls		mar 11 2014 14:15 PM
	profiles		mar 11 2014 14:15 PM
	skins		feb 20 2014 08:53 AM
	system		feb 20 2014 08:53 AM
	metadata.properties	419 b	feb 28 2014 13:11 PM
	Plain.html	3 Kb	feb 28 2014 13:11 PM
	preview.gif	8 Kb	feb 28 2014 13:11 PM
	preview.png	13 Kb	feb 28 2014 13:11 PM
	preview_rtl.gif	8 Kb	feb 28 2014 13:11 PM
	theme.html	5 Kb	feb 28 2014 13:11 PM
	theme_sidenav.html	5 Kb	feb 28 2014 13:11 PM

Una vez ubicados en el directorio que almacena los archivos estáticos (<TemaFidelizacionAval>), se debe proceder con los siguientes pasos:

1. Realizar la conexión a partir del cliente WebDAV y con credenciales de usuario administrador a la dirección del tema en el servidor:  
http://<hostname>:<port>/wps/mycontenthandler/dav/themelist/,
2. Así mismo se debe especificar el protocolo de acceso WebDAV y realizar la conexión a partir del botón Conectar:

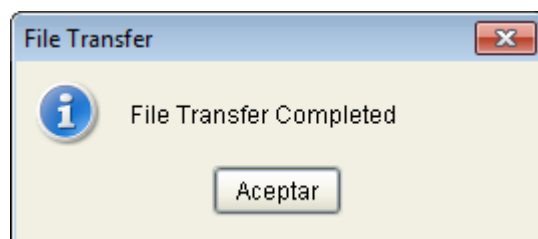


3. Una vez conectados al themelist se debe proceder a ubicar la carpeta producto de la descompresión del archivo <TemaFidelizacionAval>.zip y transferirla al directorio remoto, a partir del botón de carga, tal y como se muestra en la siguiente imagen:

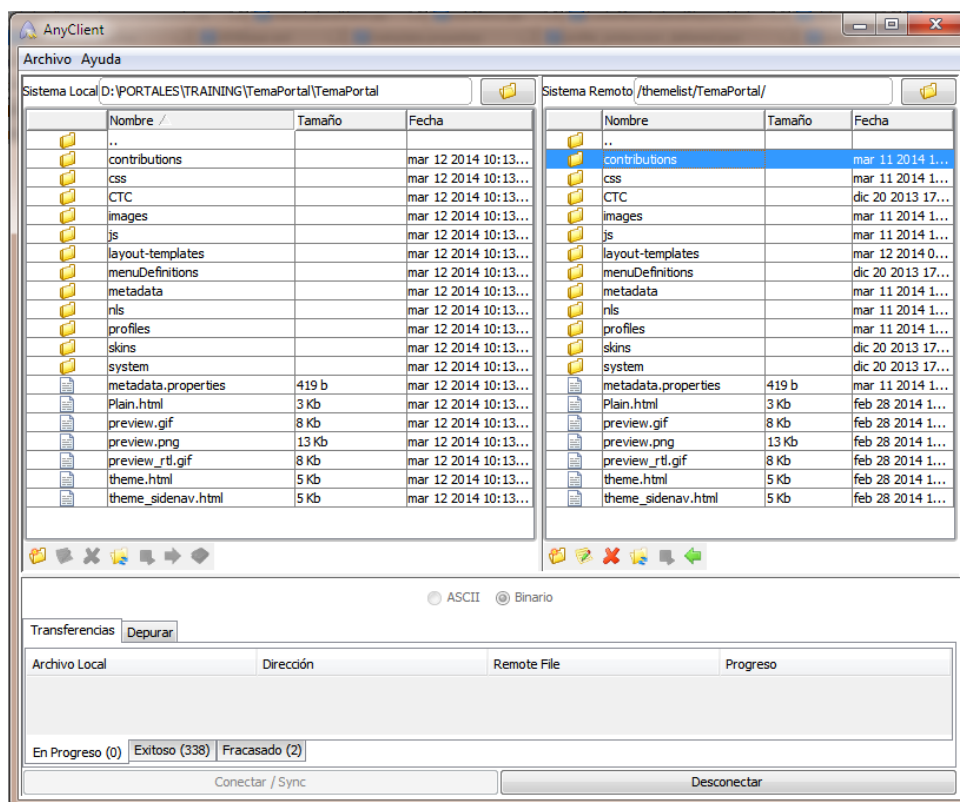



**Nota:** Como se realizó la importación del XML de temas y skins en el punto anterior, en el sistema de archivo remoto deberá aparecer una carpeta nombrada como **<TemaFidelizacionAval>** con archivos iniciales (Directorio metadata y archivo metadata.properties), en cuyo caso deben ser sobrescritos por los proporcionados en el directorio **<TemaFidelizacionAval>** del sistema de archivos local.

- El sistema confirmará que los archivos hayan sido transferidos con éxito:



- El siguiente paso contempla la verificación de que los archivos hayan sido transferidos completamente, para ello se debe validar que la estructura inicial de los archivos del directorio local coincida con la que se encuentre actualmente en el sistema remoto.



6. Se debe tener especial cuidado con los archivos css, javascript, system, layout-templates, profiles y metadata, estos son los más sensibles durante la transferencia.
7. En caso de que la transferencia falle se debe ingresar al sistema remoto del fs-type1 reemplazando /themelist por /fs-type1/themes en la ruta del sistema remoto y en caso de no existir el directorio <TemaFidelizacionAval> se debe crear a partir del ícono  con el nombre <TemaFidelizacionAval> y posteriormente transferir los archivos del directorio local a este nuevo directorio remoto.

**Nota:** Si la instalación de los temas se realiza sobre un servidor Cluster debe efectuarse sobre el nodo principal del mismo y verificar que se transfiera automáticamente a los demás nodos del cluster.

## 4. Sindicación

### 4.1. Preparación para la sindicación hacia un cluster

Cuando se necesita sindicarse hacia un servidor cluster se deben ajustar los nodos del servidor para que el servidor authoring apunte hacia el IHS y en caso de que un nodo se encuentre abajo se redirija la sindicación hacia el nodo que se encuentra arriba.

Se debe abrir la consola del **Network Deployment** del cluster y abrir la página “Environment->WebSphere Variables”

<input type="checkbox"/>	<a href="#">WCM_HOST</a>	wpsmed07	Node=wpsmed08,Server=WebSphere_Portal_2
<input type="checkbox"/>	<a href="#">WCM_HOST</a>	wpsmed07	Node=wpsmed09,Server=WebSphere_Portal
<input type="checkbox"/>	<a href="#">WCM_ILWWCM_HOME</a>	/app/IBM/PortalServer/wcm/prereq.wcm/wcm	Node=wpsmed08,Server=WebSphere_Portal_2
<input type="checkbox"/>	<a href="#">WCM_ILWWCM_HOME</a>	/app/IBM/PortalServer/wcm/prereq.wcm/wcm	Node=wpsmed09,Server=WebSphere_Portal
<input type="checkbox"/>	<a href="#">WCM_PORT</a>	80	Node=wpsmed08,Server=WebSphere_Portal_2
<input type="checkbox"/>	<a href="#">WCM_PORT</a>	80	Node=wpsmed09,Server=WebSphere_Portal

Las variables WCM\_HOST y WCM\_PORT se deben reemplazar con la ruta completa del IHS en el primer caso (fully qualified host name) y el puerto en el segundo. Estas variables existen tantos nodos tenga el cluster (En el caso de arriba se tienen dos nodos).

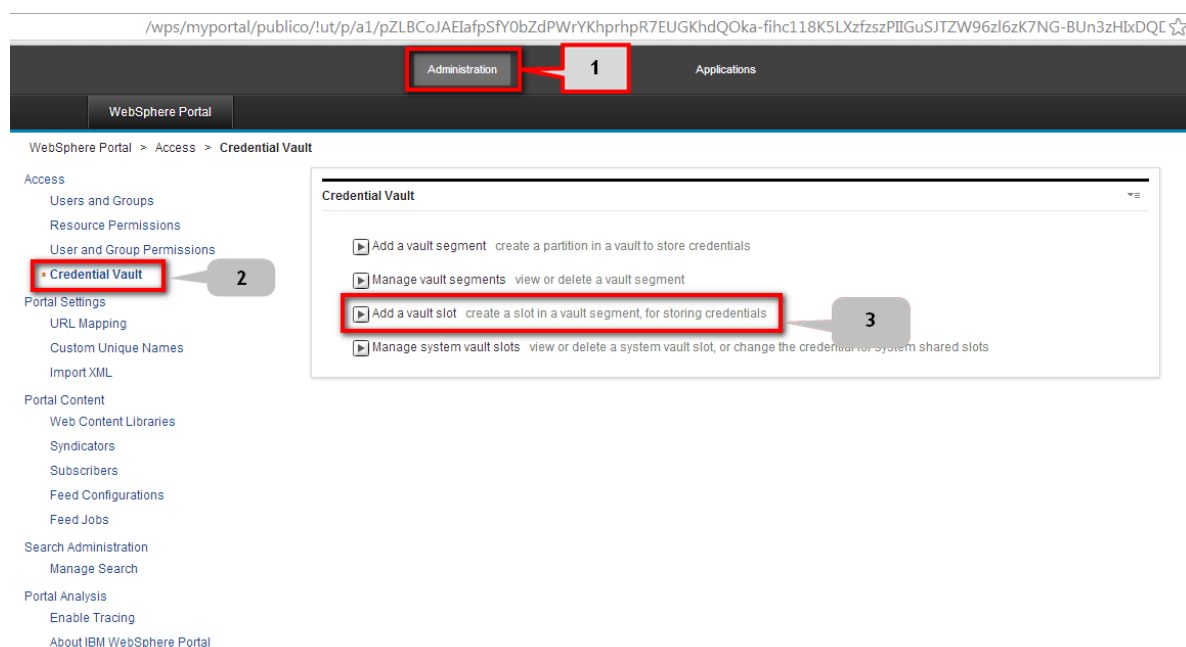
### 4.2. Procedimiento de establecimiento de la sindicación

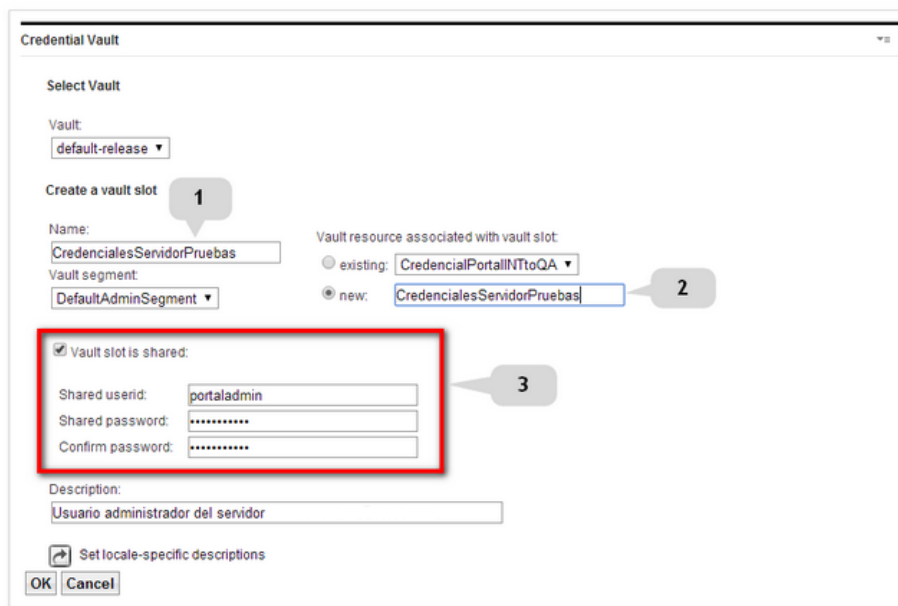
La sindicación es un mecanismo que permite compartir contenido entre dos servidores WebSphere Portal. Su ventaja frente al import es que si hay una sindicación establecida cuando un usuario crea o edita contenido en el servidor fuente, este es “Enviado” hacia el servidor de

destino sin necesidad de intervención alguna por parte de los administradores.

Se procede a almacenar las credenciales del servidor de origen en el servidor destino, si ya existe una ranura de almacenamiento con estas se puede omitir este paso. Abrir la administración del portal virtual público (/wps/myportal).

- Seleccionar la opción del menú izquierdo “almacenamiento de credenciales”.
- Seleccionar la opción “Agregar una ranura de almacenamiento”, se abre una visualización parecida a la siguiente:





Donde:

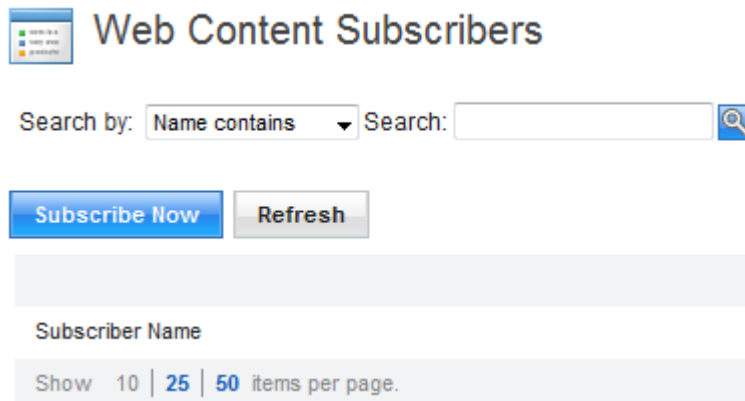
- La ranura es compartida: Esta opción debe llenarse.
- Nombre y recurso de la bóveda asociado con la ranura: Son dos nombres descriptivos que se le dan al par de credenciales y por el cual se configura la sindicación.
- En los campos de usuario y contraseña se colocan las credenciales administrativas del servidor de origen (**user:**wpadminathdev/**pass:** Pragma2013+).

Se recomienda probar la conectividad entre ambos servidores mediante ping antes de configurar la sindicación.

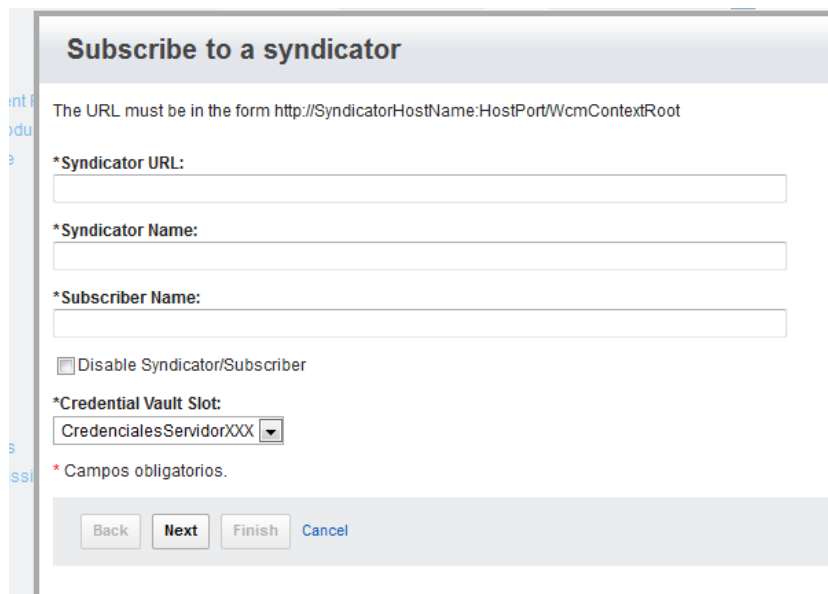
Para configurar la sindicación se debe seleccionar la opción “Suscriptores” ubicada en el lado izquierdo de la administración del portal del servidor <ServidorDestino>

Se selecciona la opción “Suscribirse ahora”





Aparece un cuadro de diálogo:



En el campo url se escribe la dirección del servidor origen:

`http://http_server/wps/wcm/portal-lealtad`

En los campos de nombre se escriben los nombres por los cuales se quiere reconocer a ambos servidores y se selecciona la ranura de la bóveda de credenciales.

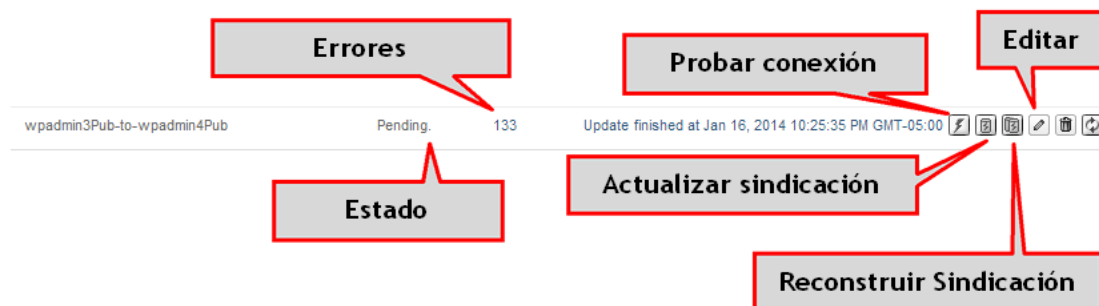
Si la conectividad y las credenciales son correctas se procede al siguiente diálogo en donde se selecciona la bibliotecas a syndicar y se escogen **todas las bibliotecas**.

Se selecciona “Finalizar” y con esta acción se establece la sindicación.

Se dirige a la vista “Suscriptores” y se espera unos segundos para pulsar el botón “Renovar” y se puede apreciar como el estado de la sindicación pasa a “Activo” y cuando la sindicación finalice

se puede ver que el campo “Última Actualización” aparece con la fecha de la finalización de la última sindicación. Al hacer clic sobre esta fecha se puede ver el reporte de actividad de cuales elementos se sindicaron.

Los botones para controlar la sindicación son los siguientes:

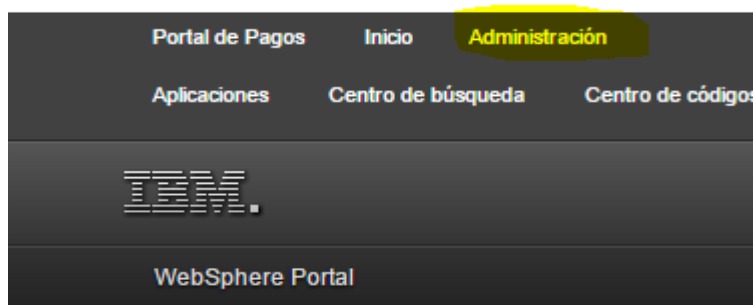


El botón de actualizar envía al servidor destino solo los elementos que se han modificado desde la última sindicación. El botón de reconstruir transfiere la biblioteca completa, lo cual es una acción que puede demorarse varios minutos y se recomienda que durante el transcurso de este no se modifique contenido en ninguno de los dos servidores.

**Nota:** Es posible que la sindicación de la biblioteca Sitio del portal (Portal Site) muestre errores relacionados con Portlets. En cuyo caso es necesario Importar todos los portlets y reintentar la sindicación de los elementos con error.

#### 4.3. Permisos en las bibliotecas de contenido

Además de ello se debe verificar que los permisos en las bibliotecas sindicadas, estén para todos los usuarios del Portal, siga los siguientes pasos:



bienvenido

Interfaz de usuario del portal

Gestionar páginas

Plantillas de páginas

Acceso

Usuarios y grupos

Permisos de recursos

Permisos de usuarios y grupos

Almacenamiento de credenciales

Valores del portal

Correlación de URL

Nombres exclusivos personalizados

Importar XML

Contenido del portal

■ **Bibliotecas de contenido web**

Sindicadores

Suscriptores

Configuraciones de canal de información

Trabajo de canal de información



Biblioteca

Buscar por:

Crear biblioteca









Nombre de biblioteca

PortalRecaudadores

Sitio del portal (Portal Site)

Mostrar: 10 | 25 | 50

Primero | Anterior | Siguiente | Último

Nombre de biblioteca	Estado	
PortalRecaudadores		   
Sitio del portal (Portal Site)		   

Mostrar: 10 | 25 | 50 elementos por página

Primero | Anterior | Siguiente | Último

Usuario	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
---------	-------------------------------------	-------------------------------------	---

**Permisos de recursos**

 **Añadir**

[Recursos](#) ▶ [Usuario](#)

[Resources](#) ▶ [User](#) ▶ **Add Role Members**

<input checked="" type="checkbox"/>	Users and User Groups
<input checked="" type="checkbox"/>	All Authenticated Portal Users
<input checked="" type="checkbox"/>	All Portal User Groups
<input checked="" type="checkbox"/>	Anonymous Portal User

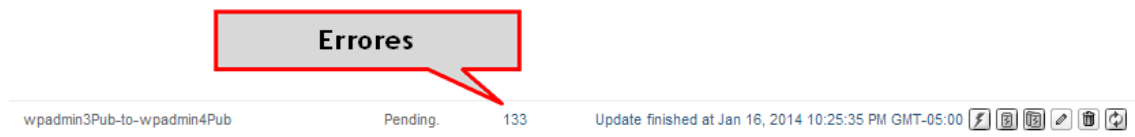
n Visualizar/Modificar propietario

Realizar este procedimiento para cada una de las bibliotecas que se van a usar en el portal.

#### 4.4. Errores comunes de la sindicación

#### 4.4.1. Elementos fallidos

La sindicación presenta elementos fallidos:



Dar clic sobre el número de elementos con error y validar los errores en el listado de elementos que presentan falla.

Algunas veces, es necesario editar los contenidos con falla y luego dar clic a Reintentar todos, para que estos puedan syndicar correctamente.

#### 4.4.2. Sindicador bloqueado

Cuando se requiere editar el sindicador y este muestra un mensaje de bloqueo por algún usuario (Generalmente por el usuario asignado a las credenciales del suscriptor), se debe dar clic sobre el enlace de desbloqueo e intentar la edición nuevamente.

#### 4.4.3. Error de conexión entre el sindicador y el suscriptor

Al probar la conexión sale el siguiente error:

IWKWC0052E: The syndicator was unable to communicate with the subscriber "suscriptor-desde-sindicador".

Es necesario ir a la edición del sindicador (Icono del lápiz) y validar la url del suscriptor:

\*Subscriber URL:

## 5. Portlets

### 5.1. Importar portlets desde el servidor (WebMod)

En el servidor de pruebas se deben copiar el contenido de la carpeta **Deployed.zip** en la ruta `<wp_profile_root>/PortalServer/deployed/archive`.

**Nota:** Se recomienda usar el comando `cp -rR`.

### 5.2. Importar portlets desde el servidor <ServidorDestino> XML

Realizar el import de los siguientes XMLs en el portal base:

- ImportPortletsDEV SP3.xml
- ImportPortletsWCM SP3.xml
- PaginaRegistro.xml

## 6. Procedimientos adicionales

### 6.1. Configuración Portlets Scripts (Angular)

Para que WebSphere Portal, no tenga inconvenientes en la integración con Angular, se deben ejecutar los siguientes pasos:

1. Ingresar al WAS a la siguiente ruta:



## 2. Ubique el WCMConfigService

Preferences

New... Delete

Select Name Scope

To filter the following table, select the column by which to filter, then enter filter

Filter Name

Search terms: \*WCMConfigService\*

Go

You can administer the following resources:

☐ WCM WCMConfigService

Total 80 Filtered total: 1

## 3. Editar las propiedades

- Additional Properties**
- Referenceables
  - Resource environment entries
  - Custom properties**

## 4. Añada las siguientes preferencias

Use this page to specify custom

Preferences

New... Delete

Preferencia: dynamic.parameter.tag.enabled

Valor: false

### General Properties

\* Scope  
cells:dmgrqaCell01:clusters:PortalCluster

\* Name  
**dynamic.parameter.tag.enabled**

Value  
false

Description  
Se añaden preferencias para integración con Angular

Type  
java.lang.String ▼

Apply **OK** Reset Cancel

**Preferencia:** renderingplugin.shortform.enabled

**Valor:** false

### General Properties

\* Scope  
cells:dmgrqaCell01:clusters:PortalCluster

\* Name  
renderingplugin.shortform.enabled

Value  
false

Description  
Se añaden preferencias para integración con Angular

Type  
java.lang.String ▼

Apply **OK** Reset Cancel

5. Guarde los cambios.
6. Realice el import del siguiente XML <<XMLParaAngular.xml>>
7. Una vez realizado estos dos procedimientos se debe reiniciar el servidor



Fuente: <https://github.com/digexp/sample-angular4-script-application>

[https://www.ibm.com/support/knowledgecenter/en/SSYJ99\\_8.5.0/wcm/prevent\\_friendly\\_url\\_redirects.html](https://www.ibm.com/support/knowledgecenter/en/SSYJ99_8.5.0/wcm/prevent_friendly_url_redirects.html)

## 6.2 outbound connections (Ajax Proxy)

Estos son los pasos para realizar el registro del ajax-proxy en WebSphere Portal 9.0

En esta guía configuraremos un servicio público, al final se dejan las fuentes para configuraciones más avanzadas como, cookies, sesiones, tokens, timeouts etc.

### 6.2.1. Correlación de servlet

La correlación de servlet consiste en habilitar un **context-path** único para nuestras peticiones, es decir, tener un contexto diferente a **/proxy** (esto también es una correlación de servlet)

En el archivo **web.xml** y **web\_merged.xml** que se encuentran en la ruta:

#### Portal:

```
<<path>>/IBM/WebSphere/wp_profile/config/cells/<<cell>>/applications/wps.ear/deployments/wps/wps.war/WEB-INF
```

#### Dmgr (Si la instalación cuenta con esta característica)

```
<<path>>/IBM/AppServer/profiles/<<dmgr01>>/config/cells/<<cell>>/applications/wps.ear/deployments/wps/wps.war/WEB-INF/
```

Adicionar las siguientes líneas

```
<!-- correlacion del servlet para invocaciones del gateway -->
<servlet-mapping>
  <servlet-name>ProxyServlet</servlet-name>
  <url-pattern>/gateway/*</url-pattern>
</servlet-mapping>
<!-- / correlacion del servlet para invocaciones del gateway -->
```

Quedando como se ve en la siguiente imagen

```

</servlet-mapping>
<servlet-mapping>
  <servlet-name>ProxyServlet</servlet-name>
  <url-pattern>/cmis_proxy/*</url-pattern>
</servlet-mapping>
<!-- correlacion del servlet para invocaciones del gateway -->
<servlet-mapping>
  <servlet-name>ProxyServlet</servlet-name>
  <url-pattern>/gateway/*</url-pattern>
</servlet-mapping>
<!-- / correlacion del servlet para invocaciones del gateway -->
<servlet-mapping>
  <servlet-name>WSDLServiceConfig</servlet-name>
  <url-pattern>/wsdl/*</url-pattern>
</servlet-mapping>

```

Reiniciar el servidor una vez configurado

**NOTA:** Este punto se realiza una única vez

### 6.2.2. Configurar el proxy

En el servidor de portal copiar el archivo config-file.xml sobre una ruta con permisos recursivos

<<path\_server>>/wp\_profile/ajax-proxy/config-file.xml (adjunto ejemplo con esta guía, si la carpeta no existe, se debe crear, esta debe tener permisos suficientes de escritura y lectura)

**NOTA:** Tener en cuenta que la ip y puertos de estos ejemplos debe de ser modificada por la del ambiente correspondiente, estas son las de kubernetes

Configurar la política que se desea agregar dentro de un mapping donde referenciaremos nuestro contextpath

```
<mapping contextpath="/gateway" url="http://10.125.63.123:1443/gateway/" name="services">
  <policy url="http://10.125.63.123:1443/gateway/*" name="gateway">
    <actions>
      <method>GET</method>
      <method>POST</method>
    </actions>
    <headers>
      <header>Authorization*</header>
      <header>Content-Type*</header>
    </headers>
    <mime-types>
      <mime-type>application/json*</mime-type>
    </mime-types>
  </policy>
</mapping>
```

### 6.2.3. Actualizar la configuración del proxy

```
<<path>>/IBM/WebSphere/ConfigEngine/
```

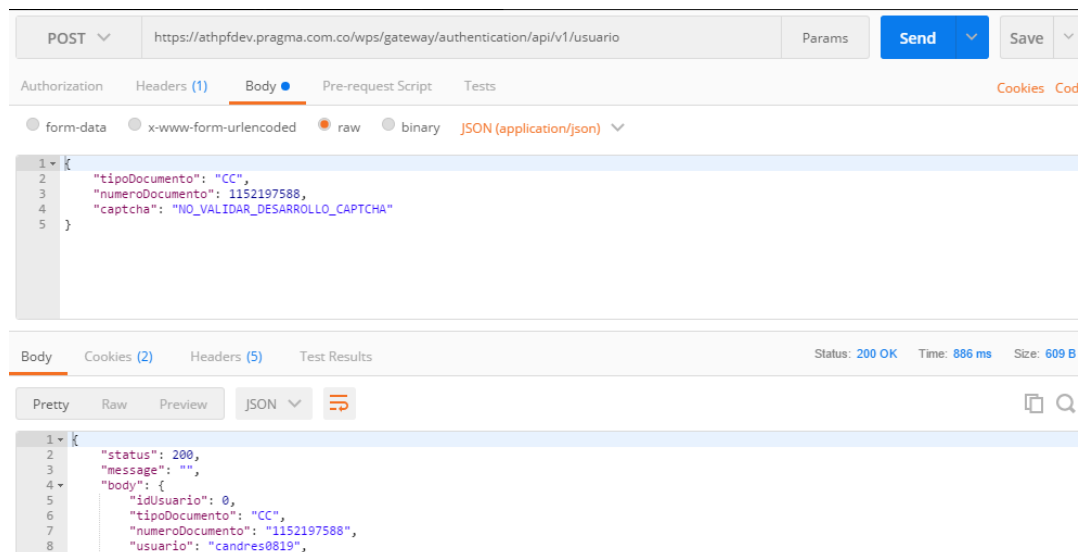
```
./ConfigEngine.sh update-outbound-http-connection-config
```

```
-DConfigFileName=<<path_server>>/ajax-proxy/config-file.xml -DWasPassword=<<psw>>
```

```
-DPortalAdminPwd=<<psw>>
```

```
cleanup-config:
  [echo] executing post-configuration tasks
BUILD SUCCESSFUL
isIsSeries currently set to: null
update-registry-sync-property:
  [echo] updated RegistrySynchronized in file wkplc.properties with value: true
print-final-message:
```

Probar la configuración consumiendo un servicio mediante el proxy



Con esto ya queda registrado el proxy, en el archivo adjunto también se encuentra la configuración del timeout global.

**NOTA:** para ambientes en clúster realizar la configuración en ambos nodos

## 6.2.4. Otros comandos utilitarios son

Limpiar las configuraciones que ya no apliquen

```
./ConfigEngine.sh clean-outbound-http-connection-config -DOutboundProfileType=global
-DWasPassword=<<psw>> -DPortalAdminPwd=<<psw>>
```

Leer las configuraciones

```
./ConfigEngine.sh read-outbound-http-connection-config
-DConfigFileName=<<path_server>>/ajax-proxy/config-file.xml -DWasPassword=<<psw>>
-DPortalAdminPwd=<<psw>>
```

Fuente para mayor información y resolver dudas: [ajax\\_proxy](#)

## 6.3. Editar preferencias de Portlets

Sobre la consola administrativa del portal (portal base), en el menú lateral, la opción de *Módulos Web*, buscar el portlet **login-portlet**

Bienvenido

Interfaz de usuario del portal

- Gestionar páginas
- Temas y skins
- Plantillas de página

Gestión de portlets

- Módulos web
- Aplicaciones
- Portlets
- Servicios web
- Gestor de aplicaciones web virtuales

Acceso

Gestionar módulos web

Buscar por:  Buscar:

**Módulo web** Pulse Instalar para instalar un módulo web. Seleccione un módulo web para ver las aplicaciones de portlets y portlets. Pulse en Suprimir para eliminar el módulo de su portal, o pulse Asignar acceso para permitir a otros que utilicen el módulo web.

Nombre	Tipo de API	Estado
login-portlet.war	JSR 286	

Página 1 de 1

Hacer clic sobre éste, y en la vista siguiente clic sobre *co.com.ath.fidelizacion.portlet.LoginPortlet*

Gestionar módulos web

Buscar por:  Buscar:

[Seleccionar módulo web](#)

**Aplicaciones de portlet** Pulse en Copiar para clonar la aplicación, Editar para cambiar las propiedades, Suprimir para eliminarlas del portal o Asignar acceso para gestionar el control de acceso.

Título	Tipo de API	Estado
co.com.ath.fidelizacion.portlet.LoginPortlet	JSR 286	

Página 1 de 1


En la vista siguiente se listaran los portlets que contiene el módulo web, a la derecha de estos dar clic sobre el icono de llave inglesa













Página 1 de 1				
Título	Tipo de API	Nombre exclusivo	Proporcionado	Estado
FD - LoginFidelizacion - (JSR286)	JSR 286			
FD - RegistroFidelizacion - (JSR286)	JSR 286			
Página 1 de 1				

Saldrá la vista de configuración y editar allí las preferencias de *endpoints* (*ips y puertos*) por los que corresponden al ambiente de la instalación (*endpoints de kubernetes*)

### Configurar portlet: FD - LoginFidelizacion - (JSR286)

**Preferencia y valores** Especifique un nuevo par preferencia/valor en los campos en blanco para crear una nueva preferencia para esta aplicación de portlet o pulse Suprimir para eliminar un par preferencia/valor. Pulse Aceptar para guardar los cambios o Cancelar para salir.

Nueva preferencia:  Nuevo valor:   **Añadir**

Página 1 de 1		
Preferencia	Valor	
captcha	6LcSSUwUAAAAAKtWl83w8HDMOWnKEBf1DKExpG-O	 
endpointAutenticacion	<a href="http://10.125.63.123:1443/gateway/authentication/api/v1/auth">http://10.125.63.123:1443/gateway/authentication/api/v1/auth</a>	 
endpointConsultaUsuario	<a href="http://10.125.63.123:1443/gateway/authentication/api/v1/usuario">http://10.125.63.123:1443/gateway/authentication/api/v1/usuario</a>	 
endpointLogout	<a href="http://10.125.63.123:1443/gateway/authentication/api/v1/logout">http://10.125.63.123:1443/gateway/authentication/api/v1/logout</a>	 
urlHome	/wps/myportal/portal-lealtad/web/inicio	 
validarCaptcha	false	 
Página 1 de 1		











## 6.3.1 Preferencia url Aviatour

Validar que el portlet cuente con las siguientes preferencias

**urlPortalViajes:** <https://portal-viajesaval.grupoaviatur.com/>

**urlPortalViajesLogged:** /wps/portal/portal-lealtad/web/inicia-sesion-externo/loggein

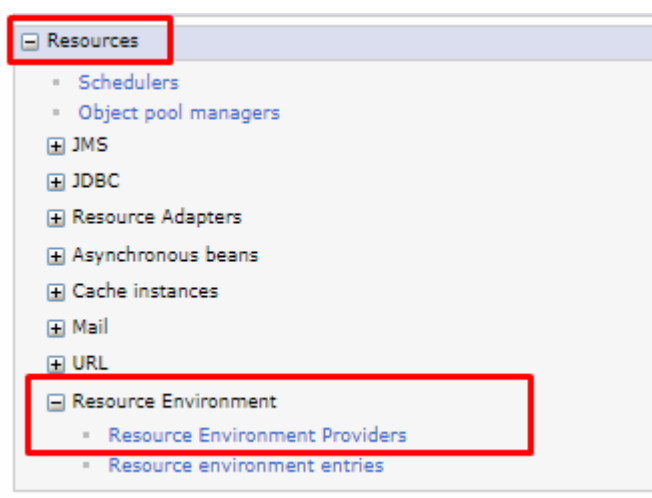
Página 1 de 1				
Título	Tipo de API	Nombre exclusivo	Proporcionado	Estado
FD - LoginFidelizacion - (JSR286)	JSR 286			   
FD - RegistroFidelizacion - (JSR286)	JSR 286			   
Página 1 de 1				

endpointLogout	http://10.125.63.123:1443/gateway/authentication/api/v1/logout	 
urlHome	/wps/myportal/portal-lealtad/web/inicio	 
urlPortalViajes	https://portal-viajesaval.grupoaviatur.com/	 
urlPortalViajesLogged	/wps/portal/portal-lealtad/web/inicia-sesion-externo/loggein	 
validarCaptcha	false	 

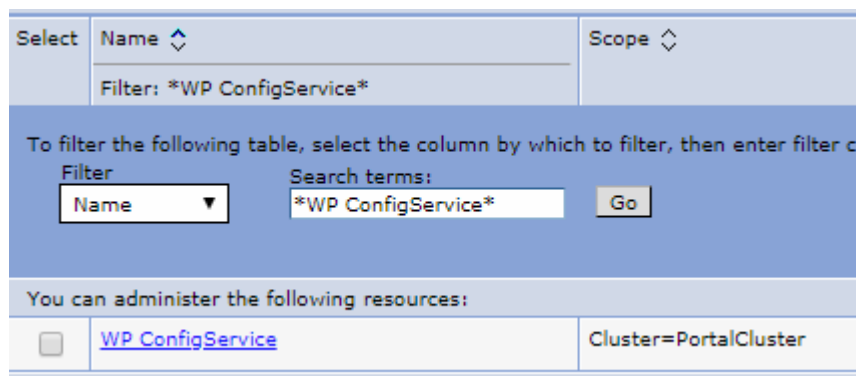
Página 1 de 1

## 6.4. Configurar preferencias en el servidor de aplicaciones

Ingresa a los Custom Properties del WP ConfigService, como lo indica la imagen:



\*WP ConfigService\*



- 
- **Additional Properties**
    - [Referenceables](#)
    - [Resource environment entries](#)
    - [Custom properties](#)

Agregue o modifique el siguiente parámetro

uri.home.substitution

true

Mantiene la sesión sin importar el contexto “portal” o “myportal”

<input type="checkbox"/>	<a href="#">uri.home.substitution</a>	true	Mantiene la sesión sin importar el contexto: "portal" o "myportal"
--------------------------	---------------------------------------	------	--

Guarde los cambios y reinicie el servidor

## 7. Anexos

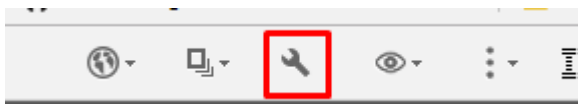
### 7.1. Configuración del idioma

Configuración del idioma del portal:

1. Ingreysar al administrador del portal
2. Realizar clic en la opción: WebSphere Portal > Valores del portal > Valores globales
3. Seleccionar español [es]. en el idioma

### 7.2. Limpieza de caché tema:

Se debe acceder a la siguiente sección





[Portal Analysis](#)

[Theme Analyzer](#)

[Enable Tracing](#)

[About IBM WebSphere Portal](#)

## Theme Optimization Analyzer

[Home](#)

# Home

*Use the analyzer to discover implementation details about your theme. For example, find contributions are used.*

### [Examine page profile information](#)

Explore pages that are arranged by site structure to view profile settings.

### [Examine modules](#)

Explore all modules in your system.

### [Examine contributions](#)

Explore modules that are arranged by contribution type to view contribution settings.

### [Examine capabilities](#) [by page](#) | [by profile](#) | [all](#)

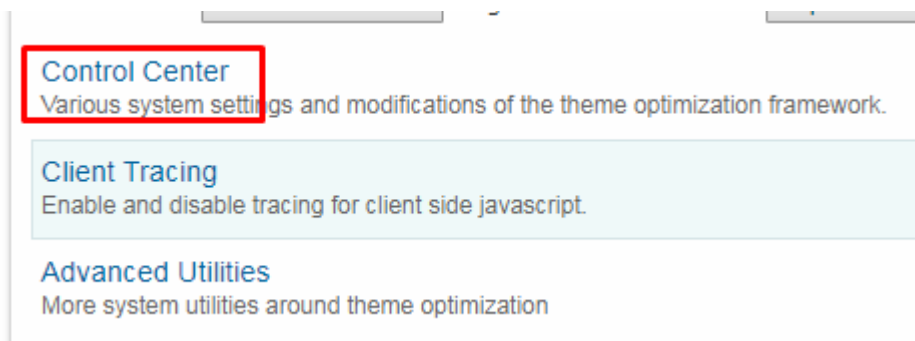
Explore all capabilities in your system.

### [Validation Report](#)

Validate your themes and their artifacts.

### [Utilities](#)

Export or import theme data as well as modify system settings and caches.



#### Invalidate Cache

This option allows to invalidate all theme optimization related caches such as profiles and modules. With this you can make changes to profiles or modules and after invalidating the caches the system will pick up the changes. [Click to invalidate.](#)

#### Remote Debugging

This option controls whether the system returns debug resources as defined by module contributions, which are usually uncompressed versions of javascript or css. This feature can be enabled for the complete server or an individual client. If the feature is enabled for the complete server, the debug resources are active for all users of this server and it stops the combiner from downloading multiple files in one request. Instead, each

**Fin del procedimiento**

### 7.3. *Permisos miga de pan*

1. Ingresar a al portal base.

<https://<nameserver>/wps/myportal/>

2. Ubicar el portlet

WebSphere Portal > Portlet Management > Portlets

Welcome

Portal User Interface

- Manage Pages
- Themes and Skins
- Page Templates

Portlet Management

- Web Modules
- Applications
- Portlets**
- Web Services
- Virtual Web Application Manager

**Manage Portlets**






Search by: **Title contains** Search: **Bread** **Search**

**Portlets** Click Copy to create a duplicate of the portlet. Click Configure to set titles, descriptions and p from your portal. Click Assign Access to allow others to work with the portlet.

Title	API Type	Unique name	Provided	Rem
Breadcrumb Trail Navigation for Static Page Aggregation	JSR 286	wps.p.SpaBreadCrumbTrail		

### 3. Ir a la opción de permisos y establecer usuario anónimo

Page 1 of 1





Title	API Type	Unique name	Provided	Remote portlet	Status
Breadcrumb Trail Navigation for Static Page Aggregation	JSR 286	wps.p.SpaBreadCrumbTrail			    

Page 1 of 1

## Permissions


### Resource Permissions

#### Breadcrumb Trail Navigation for Static Page Aggregation

Roles	Allow Inheritance	Edit Role
Administrator	✓	
Security Administrator	✓	
Manager	✓	
Editor	✓	
Privileged User	✓	
User	✓	

Display/Modify Owner

### Resource Permissions

 Add

#### Breadcrumb Trail Navigation for Static Page Aggregation ▶ User

<input checked="" type="checkbox"/>	Users and User Groups
<input checked="" type="checkbox"/>	All Authenticated Portal Users
<input checked="" type="checkbox"/>	All Portal User Groups
<input checked="" type="checkbox"/>	Anonymous Portal User

## 8. Configuración Kubernetes

### 8.0. Directorios de logs.

Crear los siguientes directorios en cada nodo del Docker (en caso de no existir) los cuales deben contar con **permisos recursivos** (lectura, escritura y edición):

- /fidaval/logs/config
- /fidaval/logs/gateway
- /fidaval/logs/authentication
- /fidaval/logs/notificaciones
- /fidaval/logs/cuenta
- /fidaval/logs/extracto
- /fidaval/logs/otp
- /fidaval/logs/redenciones

#### 8.0.1 Directorio JKS.

Crear el siguiente directorio en cada nodo de Docker (en caso de no existir) el cual debe contar con permisos recursivos (lectura, escritura y edición):

/fidaval/JKS

En el anterior directorio se debe almacenar el siguiente artefacto:

ath.jks

A continuación se detalla el método de despliegue desde las fuentes de la aplicación

### 8.1. Borrar los deployment y services ya creados

Ejecutar los siguientes comandos en kubernetes:

#### 8.1.1 config-api

*kubectrl delete deployments/config-api services/config-api*

#### 8.1.2 api-gateway

*kubectrl delete deployments/api-gateway services/api-gateway*

#### 8.1.3 authentication-api

*kubectrl delete deployments/authentication-api services/authentication-api*

#### 8.1.4 notificaciones-api

*kubectrl delete deployments/notificaciones-api services/notificaciones-api*

#### 8.1.5 cuenta-api

*kubectrl delete deployments/cuenta-api services/cuenta-api*

#### 8.1.6 extracto-api

*kubectl delete deployments/extracto-api services/extracto-api*

### **8.1.7 otp-api**

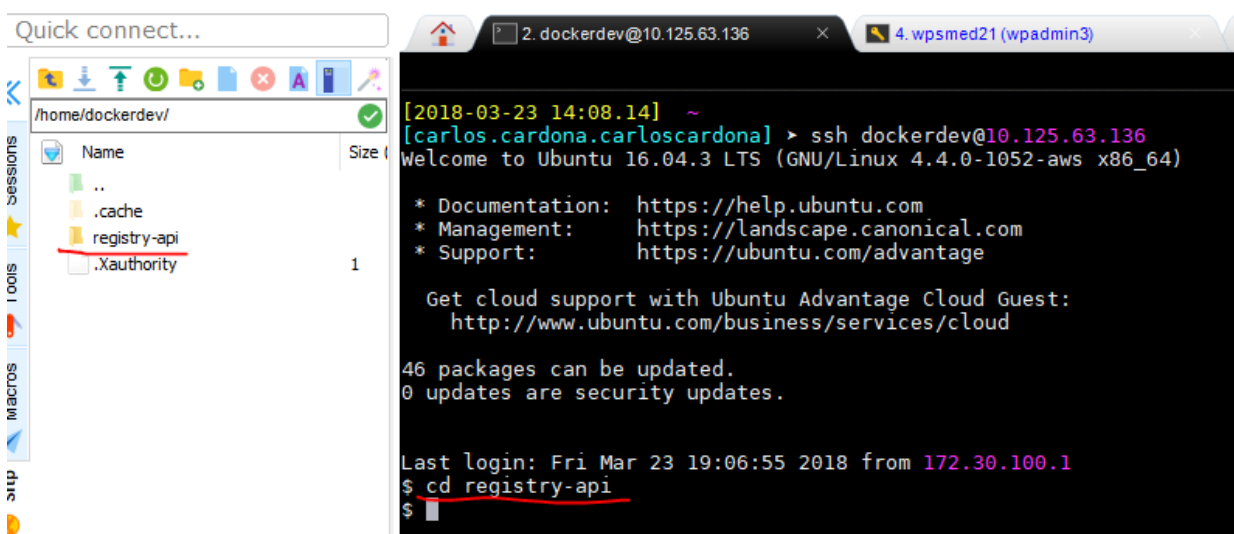
*kubectl delete deployments/otp-api services/otp-api*

### **8.1.8 redenciones-api**

*kubectl delete deployments/redenciones-api services/redenciones-api*

## 8.2. Copiar los .zip en el servidor de docker

Copiar todos los .zip que se encuentran en la ruta de repositorio en el servidor



## 8.3. Compilar las imágenes de docker

Dentro del contenedor ejecutar los siguientes comandos sobre cada uno de los contenedores (ingresar a la ruta descomprimida de cada aplicación)

- Este comando compila las imágenes a partir del Dockerfile que se encuentra en la ruta del mismo nombre (Se debe de incluir el punto)

**NOTA: CONSULTAR LA VERSIÓN DE LA API EN EL DOCUMENTO DE ENTREGA Y REEMPLAZAR LAS X.**

### 8.3.1 config-api:v

- docker build --no-cache --tag=fidelizacion/config-api:vX.X .

### 8.3.2 authentication-api:v

- docker build --no-cache --tag=fidelizacion/authentication-api:vX.X .

### 8.3.3 notificaciones-api:v

- docker build --no-cache --tag=fidelizacion/notificaciones-api:vX.X .



### 8.3.4 cuenta-api:v

- `docker build --no-cache --tag=fidelizacion/cuenta-api:vX.X .`

### 8.3.5 api-gateway:v

- `docker build --no-cache --tag=fidelizacion/api-gateway:vX.X .`

### 8.3.6 extracto-api:v

- `docker build --no-cache --tag=fidelizacion/extracto-api:vX.X .`

### 8.3.7 otp-api:v

- `docker build --no-cache --tag=fidelizacion/otp-api:vX.X .`

### 8.3.8 redenciones-api:v

- `docker build --no-cache --tag=fidelizacion/redenciones-api:vX.X .`
- Este comando crea los el Deployment y el Services en Kubernetes (dentro de cada ruta)
  - `kubectl create -f deployment.yaml`

## 8.4. Secrets

Eliminar el secret anterior con el siguiente comando:

- `kubectl delete secrets/fidelizacion-secret`

Sobre la carpeta secrets, en el archivo deployment, actualizar los valores de:

```
deployment.yaml
apiVersion: v1
data:
  datasource.url: amRiYzpvcmFjbGU6dGhpbjppAZGJtZWQxNC5wcmFnbWEuY29tLmNvOjElMjE6b3JjdXRmOA==
  datasource.user: TlJBQVRIRk1ERUxJWkFDSU9OREVW
  datasource.psw: TlJBQVRIRk1ERUxJWkFDSU9OREVW
kind: Secret
metadata:
  name: fidelizacion-secret
  namespace: default
  selfLink: /api/v1/namespaces/default/secrets/fidelizacion-secret
type: Opaque
```

Los valores deben de ser generados con los siguientes comandos en la consola de kubernetes.

## PT

url	user	psw
jdbc:oracle:thin:@10.130.3.229:1528/FIDAVAl	Fidelizacion	Proveído por TI

## QA

url	user	psw
jdbc:oracle:thin:@10.130.1.245:1528/FIDAVAl	Fidelizacion	Proveído por TI

## Comandos para PT

**Comando:** `echo -n "jdbc:oracle:thin:@10.130.3.229:1528/FIDAVAl" | base64`

**Result:** amRiYzpvcmFjbGU6dGhpbjpwMTAuMTMwLjMuMjI5OjE1MjgvRklEQVZBTA==

**Comando:** `echo -n "Fidelizacion" | base64`

**Result:** RmlkZWxpemFjaW9u

## Comandos para QA

**Comando:** `echo -n "jdbc:oracle:thin:@10.130.1.245:1528/FIDAVAl" | base64`

**Result:** amRiYzpvcmFjbGU6dGhpbjpwMTAuMTMwLjEuMjQ1OjE1MjgvRklEQVZBTA==

**Comando:** `echo -n "Fidelizacion" | base64`

**Result:** RmlkZWxpemFjaW9u

**NOTA:** Las contraseñas son suministradas por el equipo de TI y estas deben igualmente pasarse a base 64, con un comando como este:

**Comando:** `echo -n "<<ESTO LO PASA TI>>" | base64`

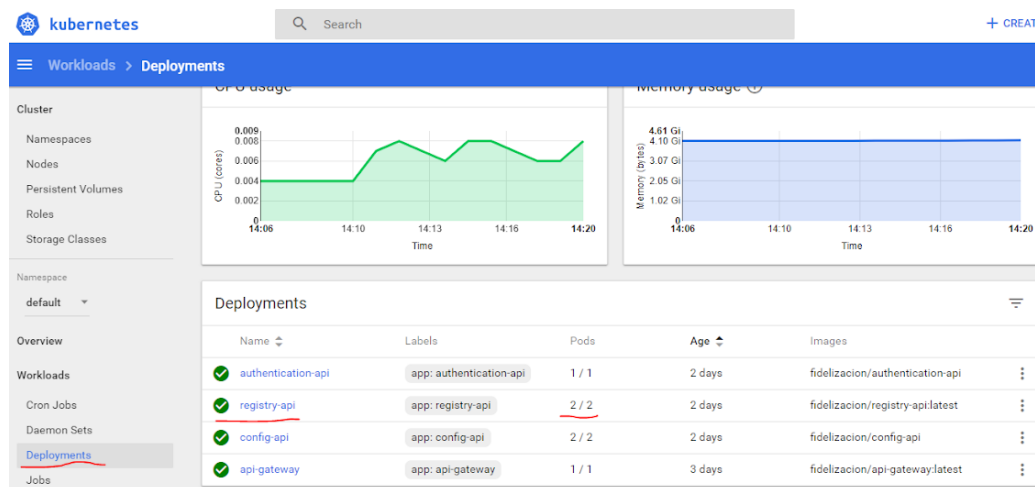
Para ambiente de **PRODUCCIÓN** no conocemos ningún valor, los comandos son los **MISMOS**

Editar los valores en el deployment y proceder con

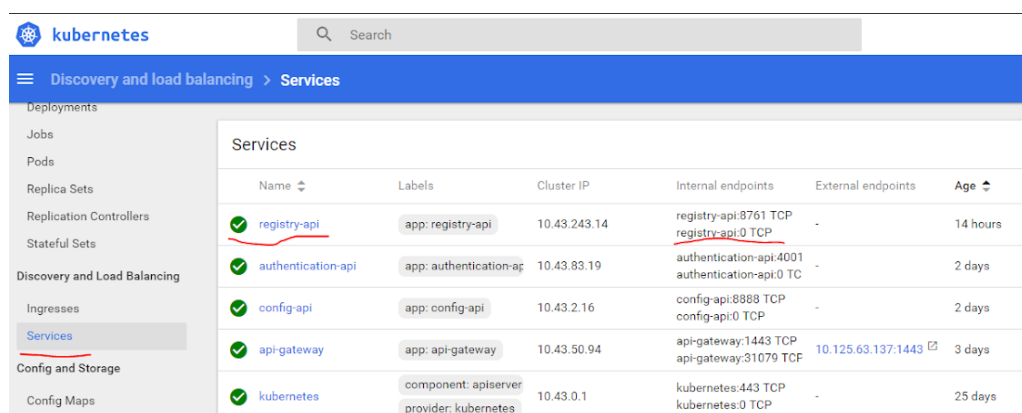
- `kubectl create -f deployment.yaml`

## 8.5. Validar que el despliegue fue correcto

Ingresa a la consola de kubernetes y validar que el deployment este así



Validar en la misma consola que el services este como en la imagen



Name	Labels	Cluster IP	Internal endpoints	External endpoints	Age
registry-api	app: registry-api	10.43.243.14	registry-api:8761 TCP registry-api:0 TCP	-	14 hours
authentication-api	app: authentication-api	10.43.83.19	authentication-api:4001 TCP authentication-api:0 TCP	-	2 days
config-api	app: config-api	10.43.2.16	config-api:8888 TCP config-api:0 TCP	-	2 days
api-gateway	app: api-gateway	10.43.50.94	api-gateway:1443 TCP api-gateway:31079 TCP	10.125.63.137:1443	3 days
kubernetes	component: apiserver provider: kubernetes	10.43.0.1	kubernetes:443 TCP kubernetes:0 TCP	-	25 days